CIS VMware vSphere 7.0 Virtual Machine STIG Benchmark

v1.0.0 - 08-21-2025

Terms of Use

Please see the below link for our current terms of use:

https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/

For information on referencing and/or citing CIS Benchmarks in 3rd party documentation (including using portions of Benchmark Recommendations) please contact CIS Legal (legalnotices@cisecurity.org) and request guidance on copyright usage.

NOTE: It is ***NEVER*** acceptable to host a CIS Benchmark in ***ANY*** format (PDF, etc.) on a 3rd party (non-CIS owned) site.

Table of Contents

Overview

Target Technology Details

VMware vSphere 7.0 Virtual Machine Secure Technical Implementation Guide (STIG)

Version: 1 Release: 4 Benchmark

Date: 30 Jan 2025

Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate VMware vSphere 7.0 Virtual Machine and are looking to comply with the STIG guidance

Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted, or the component will not be included in the recommendation.

Title

Concise description for the recommendation's intended configuration.

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile

A collection of recommendations (or rules) for securing a technology or a supporting platform. STIG Benchmark profiles are used to identify which Vulnerability Severity Category Code (CAT) each rule is associated with.

Description

The Rule Title from the STIG.

Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

Audit Procedure

Systematic instructions for determining if the target system complies with the recommendation.

Remediation Procedure

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

Additional Information

References from the STIG Rule if applicable.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **SEVERITY: CAT I**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be high severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

- **SEVERITY: CAT II**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be medium severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

- **SEVERITY: CAT III**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be low severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

Acknowledgements

The Recommendations in this Benchmark are a representation of the Rules in the unclassified DISA STIG for VMware vSphere 7.0 Virtual Machine

Recommendations

1 STIG RULES

VMware vSphere 7.0

VMware vSphere 7.0 Virtual Machine Secure Technical Implementation Guide (STIG)

Version: 1 Release: 4 Benchmark

Date: 30 Jan 2025

CLASSIFICATION unclassified

1.1 VMCH-70-000001 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Copy operations must be disabled on the virtual machine (VM).

```
GROUP ID: V-256450
RULE ID: SV-256450r959010
```

Rationale:

Copy and paste operations are disabled by default; however, explicitly disabling this feature will enable audit controls to verify this setting is correct. Copy, paste, drag and drop, or GUI copy/paste operations between the guest operating system and the remote console could provide the means for an attacker to compromise the VM.

Audit:

From the vSphere Client, right-click the Virtual Machine and go to Edit Settings >> VM Options >> Advanced >> Configuration Parameters >> Edit Configuration.

Verify the "isolation.tools.copy.disable" value is set to true.

or

From a PowerCLI command prompt while connected to the ESXi host or vCenter server, run the following command:

Get-VM "VM Name" | Get-AdvancedSetting -Name isolation.tools.copy.disable

If the virtual machine advanced setting "isolation.tools.copy.disable" does not exist or is not set to "true", this is a finding.

Remediation:

From the vSphere Client, right-click the Virtual Machine and go to Edit Settings >> VM Options >> Advanced >> Configuration Parameters >> Edit Configuration.

Find the "isolation.tools.copy.disable" value and set it to "true".

If the setting does not exist, add the Name and Value setting at the bottom of screen.

Note: The VM must be powered off to configure the advanced settings through the vSphere Client. Therefore, it is recommended to configure these settings with PowerCLI as this can be done while the VM is powered on. Settings do not take effect via either method until the virtual machine is cold started, not rebooted.

or

From a PowerCLI command prompt while connected to the ESXi host or vCenter server, run the provided commands as noted below.

If the setting does not exist, run:

Get-VM "VM Name" | New-AdvancedSetting -Name isolation.tools.copy.disable -Value true

If the setting exists, run:

Get-VM "VM Name" | Get-AdvancedSetting -Name isolation.tools.copy.disable | Set-AdvancedSetting -Value true

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.2 VMCH-70-000002 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Drag and drop operations must be disabled on the virtual machine (VM).

```
GROUP ID: V-256451
RULE ID: SV-256451r959010
```

Rationale:

Copy and paste operations are disabled by default; however, explicitly disabling this feature will enable audit controls to verify this setting is correct. Copy, paste, drag and drop, or GUI copy/paste operations between the guest operating system and the remote console could provide the means for an attacker to compromise the VM.

Audit:

From the vSphere Client, right-click the Virtual Machine and go to Edit Settings >> VM Options >> Advanced >> Configuration Parameters >> Edit Configuration.

Verify the "isolation.tools.dnd.disable" value is set to "true".

or

From a PowerCLI command prompt while connected to the ESXi host or vCenter server, run the following command:

Get-VM "VM Name" | Get-AdvancedSetting -Name isolation.tools.dnd.disable

If the virtual machine advanced setting "isolation.tools.dnd.disable" does not exist or is not set to "true", this is a finding.

Remediation:

From the vSphere Client, right-click the Virtual Machine and go to Edit Settings >> VM Options >> Advanced >> Configuration Parameters >> Edit Configuration.

Verify the "isolation.tools.dnd.disable" value is set to "true".

If the setting does not exist, add the Name and Value setting at the bottom of screen.

Note: The VM must be powered off to configure the advanced settings through the vSphere Client. Therefore, it is recommended to configure these settings with PowerCLI as this can be done while the VM is powered on. Settings do not take effect via either method until the virtual machine is cold started, not rebooted.

or

From a PowerCLI command prompt while connected to the ESXi host or vCenter server, run the provided commands as noted below.

If the setting does not exist, run:

Get-VM "VM Name" | New-AdvancedSetting -Name isolation.tools.dnd.disable -Value true

If the setting exists, run:

Get-VM "VM Name" | Get-AdvancedSetting -Name isolation.tools.dnd.disable | Set-AdvancedSetting -Value true

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.3 VMCH-70-000003 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Paste operations must be disabled on the virtual machine (VM).

```
GROUP ID: V-256452
RULE ID: SV-256452r959010
```

Rationale:

Copy and paste operations are disabled by default; however, explicitly disabling this feature will enable audit controls to verify this setting is correct. Copy, paste, drag and drop, or GUI copy/paste operations between the guest operating system and the remote console could provide the means for an attacker to compromise the VM.

Audit:

From the vSphere Client, right-click the Virtual Machine and go to Edit Settings >> VM Options >> Advanced >> Configuration Parameters >> Edit Configuration.

Verify the "isolation.tools.paste.disable" value is set to "true".

or

From a PowerCLI command prompt while connected to the ESXi host or vCenter server, run the following command:

Get-VM "VM Name" | Get-AdvancedSetting -Name isolation.tools.paste.disable

If the virtual machine advanced setting "isolation.tools.paste.disable" does not exist or is not set to "true", this is a finding.

Remediation:

From the vSphere Client, right-click the Virtual Machine and go to Edit Settings >> VM Options >> Advanced >> Configuration Parameters >> Edit Configuration.

Find the "isolation.tools.paste.disable" value and set it to "true".

If the setting does not exist, add the Name and Value setting at the bottom of screen.

Note: The VM must be powered off to configure the advanced settings through the vSphere Client. Therefore, it is recommended to configure these settings with PowerCLI as this can be done while the VM is powered on. Settings do not take effect via either method until the virtual machine is cold started, not rebooted.

or

From a PowerCLI command prompt while connected to the ESXi host or vCenter server, run the provided commands as shown below.

If the setting does not exist, run:

Get-VM "VM Name" | New-AdvancedSetting -Name isolation.tools.paste.disable -Value true

If the setting exists, run:

Get-VM "VM Name" | Get-AdvancedSetting -Name isolation.tools.paste.disable | Set-AdvancedSetting -Value true

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.4 VMCH-70-000004 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Virtual disk shrinking must be disabled on the virtual machine (VM).

```
GROUP ID: V-256453
RULE ID: SV-256453r959010
```

Rationale:

Shrinking a virtual disk reclaims unused space in it. If there is empty space in the disk, this process reduces the amount of space the virtual disk occupies on the host drive. Normal users and processes (those without root or administrator privileges) within virtual machines have the capability to invoke this procedure.

However, if this is done repeatedly, the virtual disk can become unavailable while this shrinking is being performed, effectively causing a denial of service. In most datacenter environments, disk shrinking is not done, so this feature must be disabled. Repeated disk shrinking can make a virtual disk unavailable. The capability to shrink is available to nonadministrative users operating within the VM's guest operating system.

Audit:

From the vSphere Client, right-click the Virtual Machine and go to Edit Settings >> VM Options >> Advanced >> Configuration Parameters >> Edit Configuration.

Verify the "isolation.tools.diskShrink.disable" value is set to "true".

or

From a PowerCLI command prompt while connected to the ESXi host or vCenter server, run the following command:

Get-VM "VM Name" | Get-AdvancedSetting -Name isolation.tools.diskShrink.disable

If the virtual machine advanced setting "isolation.tools.diskShrink.disable" does not exist or is not set to "true", this is a finding.

Remediation:

From the vSphere Client, right-click the Virtual Machine and go to Edit Settings >> VM Options >> Advanced >> Configuration Parameters >> Edit Configuration.

Find the "isolation.tools.diskShrink.disable" value and set it to "true".

If the setting does not exist, add the Name and Value setting at the bottom of screen.

Note: The VM must be powered off to configure the advanced settings through the vSphere Client. Therefore, it is recommended to configure these settings with PowerCLI as this can be done while the VM is powered on. Settings do not take effect via either method until the virtual machine is cold started, not rebooted.

or

From a PowerCLI command prompt while connected to the ESXi host or vCenter server, run the provided commands as shown below.

If the setting does not exist, run:

Get-VM "VM Name" | New-AdvancedSetting -Name isolation.tools.diskShrink.disable -Value true

If the setting exists, run:

Get-VM "VM Name" | Get-AdvancedSetting -Name isolation.tools.diskShrink.disable | Set-AdvancedSetting -Value true

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.5 VMCH-70-000005 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Virtual disk wiping must be disabled on the virtual machine (VM).

```
GROUP ID: V-256454
RULE ID: SV-256454r959010
```

Rationale:

Shrinking and wiping (erasing) a virtual disk reclaims unused space in it. If there is empty space in the disk, this process reduces the amount of space the virtual disk occupies on the host drive. Normal users and processes (those without root or administrator privileges) within virtual machines have the capability to invoke this procedure.

However, if this is done repeatedly, the virtual disk can become unavailable while this shrinking is being performed, effectively causing a denial of service. In most datacenter environments, disk shrinking is not done, so this feature must be disabled. Repeated disk shrinking can make a virtual disk unavailable. The capability to wipe (erase) is available to nonadministrative users operating within the VM's guest operating system.

Audit:

From the vSphere Client, right-click the Virtual Machine and go to Edit Settings >> VM Options >> Advanced >> Configuration Parameters >> Edit Configuration.

Verify the "isolation.tools.diskWiper.disable" value is set to "true".

or

From a PowerCLI command prompt while connected to the ESXi host or vCenter server, run the following command:

Get-VM "VM Name" | Get-AdvancedSetting -Name isolation.tools.diskWiper.disable

If the virtual machine advanced setting "isolation.tools.diskWiper.disable" does not exist or is not set to "true", this is a finding.

Remediation:

From the vSphere Client, right-click the Virtual Machine and go to Edit Settings >> VM Options >> Advanced >> Configuration Parameters >> Edit Configuration.

Find the "isolation.tools.diskWiper.disable" value and set it to "true".

If the setting does not exist, add the Name and Value setting at the bottom of screen.

Note: The VM must be powered off to configure the advanced settings through the vSphere Client. Therefore, it is recommended to configure these settings with PowerCLI as this can be done while the VM is powered on. Settings do not take effect via either method until the virtual machine is cold started, not rebooted.

or

From a PowerCLI command prompt while connected to the ESXi host or vCenter server, run the provided commands as shown below.

If the setting does not exist, run:

Get-VM "VM Name" | New-AdvancedSetting -Name isolation.tools.diskWiper.disable -Value true

If the setting exists, run:

Get-VM "VM Name" | Get-AdvancedSetting -Name isolation.tools.diskWiper.disable | Set-AdvancedSetting -Value true

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.6 VMCH-70-000006 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Independent, nonpersistent disks must not be used on the virtual machine (VM).

```
GROUP ID: V-256455
RULE ID: SV-256455r959010
```

Rationale:

The security issue with nonpersistent disk mode is that successful attackers, with a simple shutdown or reboot, might undo or remove any traces they were ever on the machine. To safeguard against this risk, production virtual machines should be set to use persistent disk mode; additionally, ensure activity within the VM is logged remotely on a separate server, such as a syslog server or equivalent Windows-based event collector. Without a persistent record of activity on a VM, administrators might never know whether they have been attacked or hacked.

There can be valid use cases for these types of disks, such as with an application presentation solution where read-only disks are desired, and such cases should be identified and documented.

Audit:

From the vSphere Client, right-click the Virtual Machine and go to "Edit Settings".

Review the attached hard disks and verify they are not configured as independent nonpersistent disks.

or

From a PowerCLI command prompt while connected to the ESXi host or vCenter server, run the following command:

Get-VM "VM Name" | Get-HardDisk | Select Parent, Name, Filename, DiskType, Persistence | FT -AutoSize

If the virtual machine has attached disks that are in independent nonpersistent mode and are not documented, this is a finding.

Remediation:

From the vSphere Client, right-click the Virtual Machine and go to "Edit Settings".

Select the target hard disk and change the mode to "persistent" or uncheck "Independent".

or

From a PowerCLI command prompt while connected to the ESXi host or vCenter server, run the provided commands as shown below.

Get-VM "VM Name" | Get-HardDisk | Set-HardDisk -Persistence IndependentPersistent

or

Get-VM "VM Name" | Get-HardDisk | Set-HardDisk -Persistence Persistent

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.7 VMCH-70-000007 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Host Guest File System (HGFS) file transfers must be disabled on the virtual machine (VM).

```
GROUP ID: V-256456
RULE ID: SV-256456r959010
```

Rationale:

Setting "isolation.tools.hgfsServerSet.disable" to "true" disables registration of the guest's HGFS server with the host. Application Programming Interfaces (APIs) that use HGFS to transfer files to and from the guest operating system, such as some VIX commands, will not function. An attacker could use this to transfer files inside the guest operating system.

Audit:

From the vSphere Client, right-click the Virtual Machine and go to Edit Settings >> VM Options >> Advanced >> Configuration Parameters >> Edit Configuration.

Verify the "isolation.tools.hgfsServerSet.disable" value is set to "true".

or

From a PowerCLI command prompt while connected to the ESXi host or vCenter server, run the following command:

Get-VM "VM Name" | Get-AdvancedSetting -Name isolation.tools.hgfsServerSet.disable

If the virtual machine advanced setting "isolation.tools.hgfsServerSet.disable" does not exist or is not set to "true", this is a finding.

Remediation:

From the vSphere Client, right-click the Virtual Machine and go to Edit Settings >> VM Options >> Advanced >> Configuration Parameters >> Edit Configuration.

Find the "isolation.tools.hgfsServerSet.disable" value and set it to "true".

If the setting does not exist, add the Name and Value setting at the bottom of screen.

Note: The VM must be powered off to configure the advanced settings through the vSphere Client. Therefore, it is recommended to configure these settings with PowerCLI as this can be done while the VM is powered on. Settings do not take effect via either method until the virtual machine is cold started, not rebooted.

or

From a PowerCLI command prompt while connected to the ESXi host or vCenter server, run the provided commands as shown below.

If the setting does not exist, run:

Get-VM "VM Name" | New-AdvancedSetting -Name isolation.tools.hgfsServerSet.disable -Value true

If the setting exists, run:

Get-VM "VM Name" | Get-AdvancedSetting -Name isolation.tools.hgfsServerSet.disable | Set-AdvancedSetting -Value true

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.8 VMCH-70-000008 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Unauthorized floppy devices must be disconnected on the virtual machine (VM).

```
GROUP ID: V-256457
RULE ID: SV-256457r959010
```

Rationale:

Ensure no device is connected to a virtual machine if it is not required. For example, floppy, serial, and parallel ports are rarely used for virtual machines in a data center environment, and CD/DVD drives are usually connected only temporarily during software installation.

Audit:

Floppy drives are no longer visible through the vSphere Client and must be done via the Application Programming Interface (API) or PowerCLI.

From a PowerCLI command prompt while connected to the ESXi host or vCenter server, run the following command:

Get-VM | Get-FloppyDrive | Select Parent, Name, ConnectionState

If a virtual machine has a floppy drive connected, this is a finding.

Remediation:

Floppy drives are no longer visible through the vSphere Client and must be done via the API or PowerCLI.

From a PowerCLI command prompt while connected to the ESXi host or vCenter server, run the following command:

Get-VM "VM Name" | Get-FloppyDrive | Remove-FloppyDrive

Note: The VM must be powered off to remove the floppy drive.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.9 VMCH-70-000009 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Unauthorized CD/DVD devices must be disconnected on the virtual machine (VM).

```
GROUP ID: V-256458
RULE ID: SV-256458r959010
```

Rationale:

Ensure no device is connected to a virtual machine if it is not required. For example, floppy, serial, and parallel ports are rarely used for virtual machines in a data center environment, and CD/DVD drives are usually connected only temporarily during software installation.

Audit:

From the vSphere Client, right-click the Virtual Machine and go to "Edit Settings".

Review the VM's hardware and verify no CD/DVD drives are connected.

or

From a PowerCLI command prompt while connected to the ESXi host or vCenter server, run the following command:

Get-VM | Get-CDDrive | Where {$_.extensiondata.connectable.connected -eq $true} | Select Parent,Name

If a virtual machine has a CD/DVD drive connected other than temporarily, this is a finding.

Remediation:

From the vSphere Client, right-click the Virtual Machine and go to "Edit Settings".

Select the CD/DVD drive and uncheck "Connected" and "Connect at power on" and remove any attached ISOs.

or

From a PowerCLI command prompt while connected to the ESXi host or vCenter server, run the following command:

Get-VM "VM Name" | Get-CDDrive | Set-CDDrive -NoMedia

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.10 VMCH-70-000010 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Unauthorized parallel devices must be disconnected on the virtual machine (VM).

```
GROUP ID: V-256459
RULE ID: SV-256459r959010
```

Rationale:

Ensure no device is connected to a virtual machine if it is not required. For example, floppy, serial, and parallel ports are rarely used for virtual machines in a data center environment, and CD/DVD drives are usually connected only temporarily during software installation.

Audit:

From the vSphere Client, right-click the Virtual Machine and go to "Edit Settings".

Review the VM's hardware and verify no parallel devices exist.

or

From a PowerCLI command prompt while connected to the ESXi host or vCenter server, run the following command:

Get-VM | Where {$_.ExtensionData.Config.Hardware.Device.DeviceInfo.Label -match "parallel"}

If a virtual machine has a parallel device present, this is a finding.

Remediation:

The VM must be powered off to remove a parallel device.

From the vSphere Client, right-click the Virtual Machine and go to "Edit Settings".

Select the parallel device, click the circled "X" to remove it, and click "OK".

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.11 VMCH-70-000011 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Unauthorized serial devices must be disconnected on the virtual machine (VM).

```
GROUP ID: V-256460
RULE ID: SV-256460r959010
```

Rationale:

Ensure no device is connected to a virtual machine if it is not required. For example, floppy, serial, and parallel ports are rarely used for virtual machines in a datacenter environment, and CD/DVD drives are usually connected only temporarily during software installation.

Audit:

From the vSphere Client, right-click the Virtual Machine and go to "Edit Settings".

Review the VM's hardware and verify no serial devices exist.

or

From a PowerCLI command prompt while connected to the ESXi host or vCenter server, run the following command:

Get-VM | Where {$_.ExtensionData.Config.Hardware.Device.DeviceInfo.Label -match "serial"}

If a virtual machine has a serial device present, this is a finding.

Remediation:

The VM must be powered off to remove a serial device.

From the vSphere Client, right-click the Virtual Machine and go to "Edit Settings".

Select the serial device, click the circled "X" to remove it, and click "OK".

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.12 VMCH-70-000012 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Unauthorized USB devices must be disconnected on the virtual machine (VM).

```
GROUP ID: V-256461
RULE ID: SV-256461r959010
```

Rationale:

Ensure no device is connected to a virtual machine if it is not required. For example, floppy, serial, and parallel ports are rarely used for virtual machines in a data center environment, and CD/DVD drives are usually connected only temporarily during software installation.

Audit:

From the vSphere Client, right-click the Virtual Machine and go to "Edit Settings".

Review the VM's hardware and verify no USB devices exist.

or

From a PowerCLI command prompt while connected to the ESXi host or vCenter server, run the following commands:

Get-VM | Where {$_.ExtensionData.Config.Hardware.Device.DeviceInfo.Label -match "usb"}

Get-VM | Get-UsbDevice

If a virtual machine has any USB devices or USB controllers present, this is a finding.

If USB smart card readers are used to pass smart cards through the VM console to a VM, the use of a USB controller and USB devices for that purpose is not a finding.

Remediation:

From the vSphere Client, right-click the Virtual Machine and go to "Edit Settings".

Select the USB controller, click the circled "X" to remove it, and click "OK".

or

From a PowerCLI command prompt while connected to the ESXi host or vCenter server, run the following command:

Get-VM "VM Name" | Get-USBDevice | Remove-USBDevice

Note: This will not remove the USB controller, just any connected devices.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.13 VMCH-70-000013 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Console connection sharing must be limited on the virtual machine (VM).

```
GROUP ID: V-256462
RULE ID: SV-256462r959010
```

Rationale:

By default, more than one user at a time can connect to remote console sessions. When multiple sessions are activated, each terminal window receives a notification about the new session. If an administrator in the VM logs in using a VMware remote console during their session, a nonadministrator in the VM might connect to the console and observe the administrator's actions.

Also, this could result in an administrator losing console access to a VM. For example, if a jump box is being used for an open console session and the administrator loses connection to that box, the console session remains open. Allowing two console sessions permits debugging via a shared session. For the highest security, allow only one remote console session at a time.

Audit:

From the vSphere Client, right-click the Virtual Machine and go to Edit Settings >> VM Options >> Advanced >> Configuration Parameters >> Edit Configuration.

Verify the "RemoteDisplay.maxConnections" value is set to "1".

or

From a PowerCLI command prompt while connected to the ESXi host or vCenter server, run the following command:

Get-VM "VM Name" | Get-AdvancedSetting -Name RemoteDisplay.maxConnections

If the virtual machine advanced setting "RemoteDisplay.maxConnections" does not exist or is not set to "1", this is a finding.

Remediation:

From the vSphere Client, right-click the Virtual Machine and go to Edit Settings >> VM Options >> Advanced >> Configuration Parameters >> Edit Configuration.

Find the "RemoteDisplay.maxConnections" value and set it to "1".

If the setting does not exist, add the Name and Value setting at the bottom of screen.

Note: The VM must be powered off to configure the advanced settings through the vSphere Client. Therefore, it is recommended to configure these settings with PowerCLI as this can be done while the VM is powered on. Settings do not take effect via either method until the virtual machine is cold started, not rebooted.

or

From a PowerCLI command prompt while connected to the ESXi host or vCenter server, run the provided commands as shown below.

If the setting does not exist, run:

Get-VM "VM Name" | New-AdvancedSetting -Name RemoteDisplay.maxConnections -Value 1

If the setting exists, run:

Get-VM "VM Name" | Get-AdvancedSetting -Name RemoteDisplay.maxConnections | Set-AdvancedSetting -Value 1

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.14 VMCH-70-000015 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Informational messages from the virtual machine to the VMX file must be limited on the virtual machine (VM).

```
GROUP ID: V-256463
RULE ID: SV-256463r1051422
```

Rationale:

The configuration file containing these name-value pairs is limited to a size of 1MB. If not limited, VMware tools in the guest operating system are capable of sending a large and continuous data stream to the host. This 1MB capacity should be sufficient for most cases, but this value can change if necessary.

The value can be increased if large amounts of custom information are being stored in the configuration file. The default limit is 1MB.

Audit:

From the vSphere Client, right-click the Virtual Machine and go to Edit Settings >> VM Options >> Advanced >> Configuration Parameters >> Edit Configuration.

Verify the "tools.setInfo.sizeLimit" value is set to "1048576".

or

From a PowerCLI command prompt while connected to the ESXi host or vCenter server, run the following command:

Get-VM "VM Name" | Get-AdvancedSetting -Name tools.setinfo.sizeLimit

If the virtual machine advanced setting "tools.setInfo.sizeLimit" does not exist or is not set to "1048576", this is a finding.

Remediation:

From the vSphere Client, right-click the Virtual Machine and go to Edit Settings >> VM Options >> Advanced >> Configuration Parameters >> Edit Configuration.

Find the "tools.setInfo.sizeLimit" value and set it to "1048576".

If the setting does not exist, add the Name and Value setting at the bottom of screen.

Note: The VM must be powered off to configure the advanced settings through the vSphere Client. Therefore, it is recommended to configure these settings with PowerCLI as this can be done while the VM is powered on. Settings do not take effect via either method until the virtual machine is cold started, not rebooted.

or

From a PowerCLI command prompt while connected to the ESXi host or vCenter server, run the provided commands as shown below.

If the setting does not exist, run:

Get-VM "VM Name" | New-AdvancedSetting -Name tools.setInfo.sizeLimit -Value 1048576

If the setting exists, run:

Get-VM "VM Name" | Get-AdvancedSetting -Name tools.setInfo.sizeLimit | Set-AdvancedSetting -Value 1048576

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.15 VMCH-70-000016 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Unauthorized removal, connection, and modification of devices must be prevented on the virtual machine (VM).

```
GROUP ID: V-256464
RULE ID: SV-256464r959010
```

Rationale:

In a virtual machine, users and processes without root or administrator privileges can connect or disconnect devices, such as network adaptors and CD-ROM drives, and can modify device settings. Use the virtual machine settings editor or configuration editor to remove unneeded or unused hardware devices. To use the device again, prevent a user or running process in the virtual machine from connecting, disconnecting, or modifying a device from within the guest operating system.

By default, a rogue user with nonadministrator privileges in a virtual machine can:

1. Connect a disconnected CD-ROM drive and access sensitive information on the media left in the drive.
2. Disconnect a network adaptor to isolate the virtual machine from its network, which is a denial of service.
3. Modify settings on a device.

Audit:

From the vSphere Client, right-click the Virtual Machine and go to Edit Settings >> VM Options >> Advanced >> Configuration Parameters >> Edit Configuration.

Verify the "isolation.device.connectable.disable" value is set to "true".

or

From a PowerCLI command prompt while connected to the ESXi host or vCenter server, run the following command:

Get-VM "VM Name" | Get-AdvancedSetting -Name isolation.device.connectable.disable

If the virtual machine advanced setting "isolation.device.connectable.disable" does not exist or is not set to "true", this is a finding.

Remediation:

From the vSphere Client, right-click the Virtual Machine and go to Edit Settings >> VM Options >> Advanced >> Configuration Parameters >> Edit Configuration.

Find the "isolation.device.connectable.disable" value and set it to "true".

If the setting does not exist, add the Name and Value setting at the bottom of screen.

Note: The VM must be powered off to configure the advanced settings through the vSphere Client. Therefore, it is recommended to configure these settings with PowerCLI as this can be done while the VM is powered on. Settings do not take effect via either method until the virtual machine is cold started, not rebooted.

or

From a PowerCLI command prompt while connected to the ESXi host or vCenter server, run the provided commands as shown below.

If the setting does not exist, run:

Get-VM "VM Name" | New-AdvancedSetting -Name isolation.device.connectable.disable -Value true

If the setting exists, run:

Get-VM "VM Name" | Get-AdvancedSetting -Name isolation.device.connectable.disable | Set-AdvancedSetting -Value true

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.16 VMCH-70-000017 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The virtual machine (VM) must not be able to obtain host information from the hypervisor.

```
GROUP ID: V-256465
RULE ID: SV-256465r959010
```

Rationale:

If enabled, a VM can obtain detailed information about the physical host. The default value for the parameter is FALSE. This setting should not be TRUE unless a particular VM requires this information for performance monitoring. An adversary could use this information to inform further attacks on the host.

Audit:

From the vSphere Client, right-click the Virtual Machine and go to Edit Settings >> VM Options >> Advanced >> Configuration Parameters >> Edit Configuration.

Verify the "tools.guestlib.enableHostInfo" value is set to "false".

or

From a PowerCLI command prompt while connected to the ESXi host or vCenter server, run the following command:

Get-VM "VM Name" | Get-AdvancedSetting -Name tools.guestlib.enableHostInfo

If the virtual machine advanced setting "tools.guestlib.enableHostInfo" does not exist or is not set to "false", this is a finding.

Remediation:

From the vSphere Client, right-click the Virtual Machine and go to Edit Settings >> VM Options >> Advanced >> Configuration Parameters >> Edit Configuration.

Find the "tools.guestlib.enableHostInfo" value and set it to "false".

If the setting does not exist, add the Name and Value setting at the bottom of screen.

Note: The VM must be powered off to configure the advanced settings through the vSphere Client. Therefore, it is recommended to configure these settings with PowerCLI as this can be done while the VM is powered on. Settings do not take effect via either method until the virtual machine is cold started, not rebooted.

or

From a PowerCLI command prompt while connected to the ESXi host or vCenter server, run the provided commands as shown below.

If the setting does not exist, run:

Get-VM "VM Name" | New-AdvancedSetting -Name tools.guestlib.enableHostInfo -Value false

If the setting exists, run:

Get-VM "VM Name" | Get-AdvancedSetting -Name tools.guestlib.enableHostInfo | Set-AdvancedSetting -Value false

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.17 VMCH-70-000018 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Shared salt values must be disabled on the virtual machine (VM).

```
GROUP ID: V-256466
RULE ID: SV-256466r959010
```

Rationale:

When salting is enabled (Mem.ShareForceSalting=1 or 2) to share a page between two virtual machines, both salt and the content of the page must be same. A salt value is a configurable advanced option for each virtual machine. The salt values can be specified manually in the virtual machine's advanced settings with the new option "sched.mem.pshare.salt".

If this option is not present in the virtual machine's advanced settings, the value of the "vc.uuid" option is taken as the default value. Because the "vc.uuid" is unique to each virtual machine, by default Transparent Page Sharing (TPS) happens only among the pages belonging to a particular virtual machine (Intra-VM).

Audit:

From the vSphere Client, right-click the Virtual Machine and go to Edit Settings >> VM Options >> Advanced >> Configuration Parameters >> Edit Configuration.

Verify the "sched.mem.pshare.salt" setting does not exist.

or

From a PowerCLI command prompt while connected to the ESXi host or vCenter server, run the following command:

Get-VM "VM Name" | Get-AdvancedSetting -Name sched.mem.pshare.salt

If the virtual machine advanced setting "sched.mem.pshare.salt" exists, this is a finding.

Remediation:

From the vSphere Client, right-click the Virtual Machine and go to Edit Settings >> VM Options >> Advanced >> Configuration Parameters >> Edit Configuration.

Delete the "sched.mem.pshare.salt" setting.

Note: The VM must be powered off to configure the advanced settings through the vSphere Client. Therefore, it is recommended to configure these settings with PowerCLI as this can be done while the VM is powered on. Settings do not take effect via either method until the virtual machine is cold started, not rebooted.

or

From a PowerCLI command prompt while connected to the ESXi host or vCenter server, run the following command:

Get-VM "VM Name" | Get-AdvancedSetting -Name sched.mem.pshare.salt | Remove-AdvancedSetting

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.18 VMCH-70-000019 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Access to virtual machines (VMs) through the "dvfilter" network Application Programming Interface (API) must be controlled.

```
GROUP ID: V-256467
RULE ID: SV-256467r959010
```

Rationale:

An attacker might compromise a VM by using the "dvFilter" API. Configure only VMs that need this access to use the API.

Audit:

From the vSphere Client, right-click the Virtual Machine and go to Edit Settings >> VM Options >> Advanced >> Configuration Parameters >> Edit Configuration.

Look for settings with the format "ethernet*.filter*.name".

or

From a PowerCLI command prompt while connected to the ESXi host or vCenter server, run the following command:

Get-VM "VM Name" | Get-AdvancedSetting -Name "ethernet*.filter*.name*"

If the virtual machine advanced setting "ethernet*.filter*.name" exists and dvfilters are not in use, this is a finding.

If the virtual machine advanced setting "ethernet*.filter*.name" exists and the value is not valid, this is a finding.

Remediation:

From the vSphere Client, right-click the Virtual Machine and go to Edit Settings >> VM Options >> Advanced >> Configuration Parameters >> Edit Configuration.

Look for settings with the format "ethernet*.filter*.name".

Ensure only required VMs use this setting.

Note: The VM must be powered off to configure the advanced settings through the vSphere Client. Therefore, it is recommended to configure these settings with PowerCLI as this can be done while the VM is powered on. Settings do not take effect via either method until the virtual machine is cold started, not rebooted.

or

From a PowerCLI command prompt while connected to the ESXi host or vCenter server, run the following command:

Get-VM "VM Name" | Get-AdvancedSetting -Name ethernetX.filterY.name | Remove-AdvancedSetting

Note: Change the X and Y values to match the specific setting in the organization's environment.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.19 VMCH-70-000020 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

System administrators must use templates to deploy virtual machines (VMs) whenever possible.

```
GROUP ID: V-256468
RULE ID: SV-256468r959010
```

Rationale:

Capture a hardened base operating system image (with no applications installed) in a template to ensure all VMs are created with a known baseline level of security. Use this template to create other, application-specific templates, or use the application template to deploy VMs. Manual installation of the operating system and applications into a VM introduces the risk of misconfiguration due to human or process error.

Audit:

Ask the system administrator if hardened, patched templates are used for VM creation and properly configured operating system deployments, including applications dependent and nondependent on VM-specific configurations.

If hardened, patched templates are not used for VM creation, this is a finding.

Remediation:

Create hardened VM templates to use for operating system deployments.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.20 VMCH-70-000021 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Use of the virtual machine (VM) console must be minimized.

```
GROUP ID: V-256469
RULE ID: SV-256469r959010
```

Rationale:

The VM console enables a connection to the console of a virtual machine, in effect seeing what a monitor on a physical server would show. The VM console also provides power management and removable device connectivity controls, which could allow a malicious user to bring down a VM. In addition, it impacts performance on the service console, especially if many VM console sessions are open simultaneously.

Audit:

Remote management services, such as terminal services and Secure Shell (SSH), must be used to interact with VMs.

VM console access should only be granted when remote management services are unavailable or insufficient to perform necessary management tasks.

Ask the system administrator if a VM console is used to perform VM management tasks other than for troubleshooting VM issues.

If a VM console is used to perform VM management tasks other than for troubleshooting VM issues, this is a finding.

If SSH and/or terminal management services are exclusively used to perform management tasks, this is not a finding.

Remediation:

Develop a policy prohibiting the use of a VM console for performing management services.

This policy should include procedures for the use of SSH and Terminal Management services for VM management.

Where SSH and Terminal Management services prove insufficient to troubleshoot a VM, access to the VM console may be granted temporarily.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.21 VMCH-70-000022 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The virtual machine (VM) guest operating system must be locked when the last console connection is closed.

```
GROUP ID: V-256470
RULE ID: SV-256470r959010
```

Rationale:

When accessing the VM console, the guest operating system must be locked when the last console user disconnects, limiting the possibility of session hijacking. This setting only applies to Windows-based VMs with VMware tools installed.

Audit:

From the vSphere Client, select the Virtual Machine, right-click, and go to Edit Settings >> VM Options tab >> Advanced >> Configuration Parameters >> Edit Configuration.

Find the "tools.guest.desktop.autolock" value and verify it is set to "true".

or

From a PowerCLI command prompt while connected to the ESXi host or vCenter server, run the following command:

Get-VM "VM Name" | Get-AdvancedSetting -Name tools.guest.desktop.autolock

If the virtual machine advanced setting "tools.guest.desktop.autolock" does not exist or is not set to "true", this is a finding.

If the VM is not Windows-based, this is not a finding.

Remediation:

From the vSphere Client, select the Virtual Machine, right-click and go to Edit Settings >> VM Options tab >> Advanced >> Configuration Parameters >> Edit Configuration.

Find or create the "tools.guest.desktop.autolock" value and set it to "true".

Note: The VM must be powered off to modify the advanced settings through the vSphere Client. It is recommended to configure these settings with PowerCLI as this can be done while the VM is powered on. In this case, the modified settings will not take effect until a cold boot of the VM.

or

From a PowerCLI command prompt while connected to the ESXi host or vCenter server, run the provided commands as shown below.

If the setting does not exist, run:

Get-VM "VM Name" | New-AdvancedSetting -Name tools.guest.desktop.autolock -Value true

If the setting exists, run:

Get-VM "VM Name" | Get-AdvancedSetting -Name tools.guest.desktop.autolock | Set-AdvancedSetting -Value true

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.22 VMCH-70-000023 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

All 3D features on the virtual machine (VM) must be disabled when not required.

```
GROUP ID: V-256471
RULE ID: SV-256471r959010
```

Rationale:

For performance reasons, it is recommended that 3D acceleration be disabled on virtual machines that do not require 3D functionality (e.g., most server workloads or desktops not using 3D applications).

Audit:

For each virtual machine do the following:

From the vSphere Client, right-click the virtual machine and go to Edit Settings.

Expand the "Video card" and verify the "Enable 3D Support" checkbox is unchecked.

or

From a PowerCLI command prompt while connected to the ESXi host or vCenter server, run the following command:

Get-VM "VM Name" | Get-AdvancedSetting -Name mks.enable3d

If the virtual machine advanced setting "mks.enable3d" exists and is not set to "false", this is a finding.

If the virtual machine advanced setting "mks.enable3d" does not exist, this is not a finding.

Remediation:

For each virtual machine do the following:

From the vSphere Client, right-click the virtual machine and go to "Edit Settings".

Expand the "Video card" and uncheck the "Enable 3D Support" checkbox.

Click "OK".

or

From a PowerCLI command prompt while connected to the ESXi host or vCenter server, run the provided commands as noted below.

If the setting does not exist, run:

Get-VM "VM Name" | New-AdvancedSetting -Name mks.enable3d -Value false

If the setting exists, run:

Get-VM "VM Name" | Get-AdvancedSetting -Name mks.enable3d | Set-AdvancedSetting -Value false

Note: The VM must be powered off to configure the advanced settings through the vSphere Client. Therefore, it is recommended to configure these settings with PowerCLI as this can be done while the VM is powered on. Settings do not take effect via either method until the virtual machine is cold started, not rebooted.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.23 VMCH-70-000024 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Encryption must be enabled for vMotion on the virtual machine (VM).

```
GROUP ID: V-256472
RULE ID: SV-256472r959010
```

Rationale:

vMotion migrations in vSphere 6.0 and earlier transferred working memory and CPU state information in clear text over the vMotion network. As of vSphere 6.5, this transfer can be transparently encrypted using 256-bit AES-GCM with negligible performance impact.

vSphere enables encrypted vMotion by default as "Opportunistic", meaning that encrypted channels are used where supported but the operation will continue in plain text where encryption is not supported.

For example, when vMotioning between two hosts, encryption will always be used. However, because 6.0 and earlier releases do not support this feature, vMotion from a 7.0 host to a 6.0 host would be allowed but would not be encrypted. If the encryption is set to "Required", vMotions to unsupported hosts will fail. This must be set to "Opportunistic" or "Required".

Audit:

From the vSphere Client, select the virtual machine, right-click, and go to Edit Settings >> VM Options tab >> Encryption >> Encrypted vMotion.

or

From a PowerCLI command prompt while connected to the ESXi host or vCenter server, run the following command:

Get-VM | Where {($_.ExtensionData.Config.MigrateEncryption -eq "disabled")}

If the setting does not have a value of "Opportunistic" or "Required", this is a finding.

Remediation:

From the vSphere Client, select the Virtual Machine, right-click, and go to Edit Settings >> VM Options tab >> Encryption >> Encrypted vMotion.

Set the value to "Opportunistic" or "Required".

or

From a PowerCLI command prompt while connected to the ESXi host or vCenter server, run the following commands:

$spec = New-Object VMware.Vim.VirtualMachineConfigSpec

$spec.MigrateEncryption = New-Object VMware.Vim.VirtualMachineConfigSpecEncryptedVMotionModes

$spec.MigrateEncryption = $true

(Get-VM -Name).ExtensionData.ReconfigVM($spec)

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.24 VMCH-70-000025 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Logging must be enabled on the virtual machine (VM).

```
GROUP ID: V-256473
RULE ID: SV-256473r959010
```

Rationale:

The ESXi hypervisor maintains logs for each individual VM by default. These logs contain information including but not limited to power events, system failure information, tools status and activity, time sync, virtual hardware changes, vMotion migrations and machine clones. Due to the value these logs provide for the continued availability of each VM and potential security incidents, these logs must be enabled.

Audit:

From the vSphere Client, select the Virtual Machine, right-click, and go to Edit Settings >> VM Options tab >> Advanced >> Settings.

Ensure that the checkbox next to "Enable logging" is checked.

or

From a PowerCLI command prompt while connected to the ESXi host or vCenter server, run the following command:

Get-VM | Where {$_.ExtensionData.Config.Flags.EnableLogging -ne "True"}

If logging is not enabled, this is a finding.

Remediation:

From the vSphere Client, select the Virtual Machine, right-click, and go to Edit Settings >> VM Options tab >> Advanced >> Settings.

Click the checkbox next to "Enable logging". Click "OK".

or

From a PowerCLI command prompt while connected to the ESXi host or vCenter server, run the following commands:

$spec = New-Object VMware.Vim.VirtualMachineConfigSpec

$spec.Flags = New-Object VMware.Vim.VirtualMachineFlagInfo

$spec.Flags.enableLogging = $true

(Get-VM -Name).ExtensionData.ReconfigVM($spec)

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.25 VMCH-70-000026 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Log size must be configured properly on the virtual machine (VM).

```
GROUP ID: V-256474
RULE ID: SV-256474r959010
```

Rationale:

The ESXi hypervisor maintains logs for each individual VM by default. These logs contain information including but not limited to power events, system failure information, tools status and activity, time sync, virtual hardware changes, vMotion migrations, and machine clones.

By default, the size of these logs is unlimited, and they are only rotated on vMotion or power events. This can cause storage issues at scale for VMs that do not vMotion or power cycle often.

Audit:

From the vSphere Client, select the Virtual Machine, right-click, and go to Edit Settings >> VM Options tab >> Advanced >> Configuration Parameters >> Edit Configuration.

Find the "log.rotateSize" value and verify it is set to "2048000".

or

From a PowerCLI command prompt while connected to the ESXi host or vCenter server, run the following command:

Get-VM "VM Name" | Get-AdvancedSetting -Name log.rotateSize

If the virtual machine advanced setting "log.rotateSize" does not exist or is not set to "2048000", this is a finding.

Remediation:

From the vSphere Client, select the Virtual Machine, right-click, and go to Edit Settings >> VM Options tab >> Advanced >> Configuration Parameters >> Edit Configuration.

Find the "log.rotateSize" value and set it to "2048000".

Note: The VM must be powered off to modify the advanced settings through the vSphere Client. It is recommended to configure these settings with PowerCLI as this can be done while the VM is powered on. In this case, the modified settings will not take effect until a cold boot of the VM.

or

From a PowerCLI command prompt while connected to the ESXi host or vCenter server, run the provided commands as shown below.

If the setting does not exist, run:

Get-VM "VM Name" | New-AdvancedSetting -Name log.rotateSize -Value 2048000

If the setting exists, run:

Get-VM "VM Name" | Get-AdvancedSetting -Name log.rotateSize | Set-AdvancedSetting -Value 2048000

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.26 VMCH-70-000027 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Log retention must be configured properly on the virtual machine (VM).

```
GROUP ID: V-256475
RULE ID: SV-256475r959010
```

Rationale:

The ESXi hypervisor maintains logs for each individual VM by default. These logs contain information including but not limited to power events, system failure information, tools status and activity, time sync, virtual hardware changes, vMotion migrations, and machine clones.

By default, 10 of these logs are retained. This is normally sufficient for most environments, but this configuration must be verified and maintained.

Audit:

From the vSphere Client, select the Virtual Machine, right-click, and go to Edit Settings >> VM Options tab >> Advanced >> Configuration Parameters >> Edit Configuration.

Find the "log.keepOld" value and verify it is set to "10".

or

From a PowerCLI command prompt while connected to the ESXi host or vCenter server, run the following command:

Get-VM "VM Name" | Get-AdvancedSetting -Name log.keepOld

If the virtual machine advanced setting "log.keepOld" is not set to "10", this is a finding.

If the virtual machine advanced setting "log.keepOld" does not exist, this is not a finding.

Remediation:

From the vSphere Client, select the Virtual Machine, right-click and go to Edit Settings >> VM Options tab >> Advanced >> Configuration Parameters >> Edit Configuration.

Find the "log.keepOld" value and set it to "10".

Note: The VM must be powered off to modify the advanced settings through the vSphere Client. It is recommended to configure these settings with PowerCLI as this can be done while the VM is powered on. In this case, the modified settings will not take effect until a cold boot of the VM.

or

From a PowerCLI command prompt while connected to the ESXi host or vCenter server, run the provided commands as shown below.

If the setting does not exist, run:

Get-VM "VM Name" | New-AdvancedSetting -Name log.keepOld -Value 10

If the setting exists, run:

Get-VM "VM Name" | Get-AdvancedSetting -Name log.keepOld | Set-AdvancedSetting -Value 10

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.27 VMCH-70-000028 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

DirectPath I/O must be disabled on the virtual machine (VM) when not required.

```
GROUP ID: V-256476
RULE ID: SV-256476r959010
```

Rationale:

VMDirectPath I/O (PCI passthrough) enables direct assignment of hardware PCI functions to VMs. This gives the VM access to the PCI functions with minimal intervention from the ESXi host. This is a powerful feature for legitimate applications such as virtualized storage appliances, backup appliances, dedicated graphics, etc., but it also allows a potential attacker highly privileged access to underlying hardware and the PCI bus.

Audit:

From the vSphere Client, select the Virtual Machine, right-click, and go to Edit Settings >> VM Options tab >> Advanced >> Configuration Parameters >> Edit Configuration.

Find any "pciPassthruX.present" value (where "X" is a count starting at 0) and verify it is set to "FALSE" or "".

or

From a PowerCLI command prompt while connected to the ESXi host or vCenter server, run the following command:

Get-VM "VM Name" | Get-AdvancedSetting -Name "pciPassthru*.present" | Select Entity, Name, Value

If the virtual machine advanced setting "pciPassthruX.present" is present, and the specific device returned is not approved, this is a finding.

If the virtual machine advanced setting "pciPassthruX.present" is not present, this is not a finding.

Remediation:

From the vSphere Client, select the Virtual Machine, right-click, and go to Edit Settings >> Virtual Hardware tab.

Find the unexpected PCI device returned from the check.

Hover the mouse over the device and click the circled "X" to remove the device. Click "OK".

or

From a PowerCLI command prompt while connected to the ESXi host or vCenter server, run the following command:

Get-VM "VM Name" | Get-AdvancedSetting -Name pciPassthruX.present | Remove-AdvancedSetting

Note: Change the "X" value to match the specific setting in the organization's environment.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.28 VMCH-70-000029 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Encryption must be enabled for Fault Tolerance on the virtual machine (VM).

```
GROUP ID: V-256477
RULE ID: SV-256477r959010
```

Rationale:

Fault Tolerance log traffic can be encrypted. This could contain sensitive data from the protected machine's memory or CPU instructions.

vSphere Fault Tolerance performs frequent checks between a primary VM and secondary VM so the secondary VM can quickly resume from the last successful checkpoint. The checkpoint contains the VM state that has been modified since the previous checkpoint.

When Fault Tolerance is turned on, FT encryption is set to "Opportunistic" by default, which means it enables encryption only if both the primary and secondary host are capable of encryption.

Audit:

If the VM does not have Fault Tolerance enabled, this is not applicable.

From the vSphere Client, select the Virtual Machine, right-click, and go to Edit Settings >> VM Options tab >> Encryption >> Encrypted FT.

or

From a PowerCLI command prompt while connected to the ESXi host or vCenter server, run the following command:

Get-VM | Where {$_.ExtensionData.Config.FtEncryptionMode -eq "ftEncryptionDisabled"}

If the setting does not have a value of "Opportunistic" or "Required", this is a finding.

Remediation:

From the vSphere Client, select the Virtual Machine, right-click, and go to Edit Settings >> VM Options tab >> Encryption >> FT Encryption.

Set the value to "Opportunistic" or "Required".

or

From a PowerCLI command prompt while connected to the ESXi host or vCenter server, run the following commands:

$spec = New-Object VMware.Vim.VirtualMachineConfigSpec

$spec.FTEncryption = New-Object VMware.Vim.VMware.Vim.VirtualMachineConfigSpecEncryptedFtModes

$spec.FT = ftEncryptionOpportunistic or ftEncryptionRequired

(Get-VM -Name).ExtensionData.ReconfigVM($spec)

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**STIG RULES**		
1.1	VMCH-70-000001 (Manual)	☐	☐
1.2	VMCH-70-000002 (Manual)	☐	☐
1.3	VMCH-70-000003 (Manual)	☐	☐
1.4	VMCH-70-000004 (Manual)	☐	☐
1.5	VMCH-70-000005 (Manual)	☐	☐
1.6	VMCH-70-000006 (Manual)	☐	☐
1.7	VMCH-70-000007 (Manual)	☐	☐
1.8	VMCH-70-000008 (Manual)	☐	☐
1.9	VMCH-70-000009 (Manual)	☐	☐
1.10	VMCH-70-000010 (Manual)	☐	☐
1.11	VMCH-70-000011 (Manual)	☐	☐
1.12	VMCH-70-000012 (Manual)	☐	☐
1.13	VMCH-70-000013 (Manual)	☐	☐
1.14	VMCH-70-000015 (Manual)	☐	☐
1.15	VMCH-70-000016 (Manual)	☐	☐
1.16	VMCH-70-000017 (Manual)	☐	☐
1.17	VMCH-70-000018 (Manual)	☐	☐
1.18	VMCH-70-000019 (Manual)	☐	☐
1.19	VMCH-70-000020 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.20	VMCH-70-000021 (Manual)	☐	☐
1.21	VMCH-70-000022 (Manual)	☐	☐
1.22	VMCH-70-000023 (Manual)	☐	☐
1.23	VMCH-70-000024 (Manual)	☐	☐
1.24	VMCH-70-000025 (Manual)	☐	☐
1.25	VMCH-70-000026 (Manual)	☐	☐
1.26	VMCH-70-000027 (Manual)	☐	☐
1.27	VMCH-70-000028 (Manual)	☐	☐
1.28	VMCH-70-000029 (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
Aug 21, 2025	1.0.0	Initial CIS Release